WHAT IS CLAIMED IS:

1. A device for use in a communication system including a transmitter, a receiver, and a serial communication link between the transmitter and the receiver, wherein the system is configured to implement a content protection protocol, the protocol requires that each of the transmitter and the receiver has a distinctive value allocated thereto, and the protocol requires that each of the transmitter and the receiver must receive the distinctive value allocated to the other of the transmitter and the receiver during an authentication procedure, wherein said device includes:

circuitry coupled and configured to compare, during the authentication procedure, the distinctive values allocated to the transmitter and the receiver, and to prevent authentication from succeeding if the distinctive values are equal.

2. The device of claim 1, wherein a first distinctive value is allocated to the transmitter, a second distinctive value is allocated to the receiver, the protocol requires that the transmitter send the first distinctive value to the receiver and that the receiver send the second distinctive value to the transmitter during the authentication procedure, and wherein the device is coupled and configured to compare the first distinctive value and the second distinctive value during the authentication procedure, and to prevent the authentication from succeeding if the first distinctive value is equal to the second distinctive value.

3. A transmitter for use in a communication system including the transmitter, a receiver, and a serial communication link between the transmitter and the receiver, wherein the system is configured to implement a content protection protocol, the protocol requires that each of the transmitter and the receiver has a distinctive value allocated thereto, a first distinctive value is allocated to the transmitter, a second distinctive value is allocated to the receiver, and the protocol requires that the transmitter send the first distinctive value to the receiver and that the receiver send the second distinctive value to the transmitter during an authentication procedure, wherein said transmitter includes:

an input configured to be coupled to the link for receiving the second distinctive value; and

circuitry coupled to the input, configured to compare the second distinctive value received at the input and the first distinctive value, and configured to prevent

authentication from succeeding if the first distinctive value is equal to the second distinctive value.

4. A receiver for use in a communication system including the receiver, a transmitter, and a serial communication link between the transmitter and the receiver, wherein the system is configured to implement a content protection protocol, the protocol requires that each of the transmitter and the receiver has a distinctive value allocated thereto, a first distinctive value is allocated to the transmitter, a second distinctive value is allocated to the receiver, and the protocol requires that the transmitter send the first distinctive value to the receiver and that the receiver send the second distinctive value to the transmitter during an authentication procedure, wherein said receiver includes:

an input configured to be coupled to the link for receiving the first distinctive value; and

circuitry coupled to the input, configured to compare the first distinctive value received at the input and the second distinctive value, and configured to prevent authentication from succeeding if the first distinctive value is equal to the second distinctive value.

5. A communication system including:

a transmitter;

a receiver; and

a serial communication link between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol, wherein the protocol requires that the transmitter send a first distinctive value to the receiver during an authentication procedure, and that the receiver send a second distinctive value to the transmitter during the authentication procedure, wherein the transmitter is configured to compare the first distinctive value with the second distinctive value received during the authentication procedure and to prevent authentication from succeeding if the first distinctive value is equal to the second distinctive value, and wherein the receiver is configured to compare the second distinctive value with the first distinctive value received during the authentication procedure and to prevent authentication from succeeding if the second distinctive value is equal to the first distinctive value.

6. A device for use in a communication system including a transmitter, a receiver, and a serial communication link between the transmitter and the receiver, wherein the system is configured to implement a content protection protocol, wherein the protocol requires that each of the transmitter and the receiver store a set of private keys, and process the private keys together with a value received from another element of the system to generate a shared secret, and wherein said device includes:

circuitry configured to check that the private keys to be processed by at least one of the transmitter and the receiver to generate the shared secret satisfy at least one predetermined criterion, and to abort generation of the shared secret if said private keys do not satisfy each said criterion.

7. The device of claim 6, wherein the at least one criterion specifies at least that none of the private keys consists entirely of ones, entirely of zeroes, or of an alternating pattern of ones and zeroes.

8. The device of claim 7, wherein the at least one criterion also specifies that none of the private keys consists of at least one other simple or regular pattern of ones and zeroes.

9. A transmitter for use in a communication system including the transmitter, a receiver, and a serial communication link between the transmitter and the receiver, wherein the system is configured to implement a content protection protocol, wherein the protocol requires that each of the transmitter and the receiver store a set of private keys, and process the private keys together with a value received from another element of the system to generate a shared secret, and wherein said transmitter includes:

circuitry configured to check that the private keys that the transmitter will process to generate the shared secret satisfy at least one predetermined criterion, and to abort generation of the shared secret if said private keys do not satisfy each said criterion.

10. The transmitter of claim 9, wherein the at least one criterion specifies at least that none of the private keys consists entirely of ones, entirely of zeroes, or of an alternating pattern of ones and zeroes.

11. A receiver for use in a communication system including the receiver, a transmitter, and a serial communication link between the transmitter and the receiver, wherein the system is configured to implement a content protection protocol, wherein the protocol requires that each of the transmitter and the receiver store a set of private keys, and process the private keys together with a value received from another element of the system to generate a shared secret, and wherein said receiver includes:

circuitry configured to check that the private keys that the receiver will process to generate the shared secret satisfy at least one predetermined criterion, and to abort generation of the shared secret if said private keys do not satisfy each said criterion.

12. The receiver of claim 11, wherein the at least one criterion specifies at least that none of the private keys consists entirely of ones, entirely of zeroes, or of an alternating pattern of ones and zeroes.

13. A communication system including:

a transmitter;

a receiver;

a serial communication link between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol, wherein the protocol requires that each of the transmitter and the receiver has private keys stored therein, that each of the transmitter and the receiver is operable in a shared secret generation mode in which it processes the private keys stored therein to generate a shared secret, and that the transmitter and the receiver must successfully complete an authentication procedure before the receiver begins to operate in its shared secret generation mode; and

an external agent configured to be coupled to at least one of the transmitter and the receiver, wherein said at least one of the transmitter and the receiver is configured to send at least one signal to the external agent when said external agent is coupled to said at least one of the transmitter and the receiver, and

wherein the external agent is configured to respond to said at least one signal by performing at least one function essential for successful completion of the authorization procedure.

14. The system of claim 13, wherein said at least one function is a system configuration verification function.

15. The system of claim 13, wherein the at least one signal is indicative of at least one of the private keys to be processed to generate the shared secret, and the external agent is configured to respond to said at least one signal by determining whether said private keys to be processed to generate the shared secret satisfy at least one predetermined criterion, and to cause said one of the transmitter and the receiver to abort generation of the shared secret if said private keys to be processed do not satisfy each said criterion.

16. The system of claim 13, wherein the at least one signal is indicative of at least one characteristic of the private keys to be processed to generate the shared secret, and the external agent is configured to respond to said at least one signal by determining whether said private keys to be processed to generate the shared secret satisfy at least one predetermined criterion, and to cause said one of the transmitter and the receiver to abort generation of the shared secret if said private keys to be processed do not satisfy each said criterion.

17. A communication system including:

a transmitter;

a receiver;

a serial communication link between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol, wherein the protocol requires that each of the transmitter and the receiver store a set of private keys, and process the private keys to generate a shared secret; and

an external agent configured to be coupled to at least one of the transmitter and the receiver, wherein said at least one of the transmitter and the receiver is configured to send a signal to the external agent when said external agent is coupled to said at least one of the transmitter and the receiver, the signal is indicative of at least one characteristic of the keys to be processed by said at least one of the transmitter and the receiver to generate the shared secret, and the external agent is configured to respond to said signal by at least one of: attempting to verify said keys to be processed to generate the shared secret, and sending information to said at least one of the transmitter and the

receiver to enable said at least one of the transmitter and the receiver to verify said keys to be processed to generate the shared secret.

18. The system of claim 17, wherein the external agent is configured to respond to the signal by attempting to verify said keys to be processed to generate the shared secret and causing said one of the transmitter and the receiver to abort generation of the shared secret unless said external agent verifies said keys to be processed.

19. A communication system including:

a transmitter;

a receiver;

a serial communication link between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol, wherein the protocol requires that each of the transmitter and the receiver store a set of private keys, and process the private keys to generate a shared secret; and

an external agent configured to be coupled to at least one of the transmitter and the receiver, wherein said at least one of the transmitter and the receiver is configured to send a verification request to the external agent when said external agent is coupled to said at least one of the transmitter and the receiver, the verification request is a request for verification of the keys to be processed by said at least one of the transmitter and the receiver to generate the shared secret, and the external agent is configured to respond to said verification request by at least one of: attempting to verify said keys to be processed to generate the shared secret, and sending information to said at least one of the transmitter and the receiver to enable said at least one of the transmitter and the receiver to verify said keys to be processed to generate the shared secret.

20. The system of claim 19, wherein the external agent is configured to respond to the verification request by attempting to verify said keys to be processed to generate the shared secret and causing said one of the transmitter and the receiver to abort generation of the shared secret unless said external agent verifies said keys to be processed.

21. A communication system including:

a transmitter;

a receiver;

a serial communication link between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol, the protocol requires that each of the transmitter and the receiver store a set of private keys and process said private keys to generate a shared secret, and at least one of the transmitter and the receiver stores an encrypted set of keys; and

an external agent configured to be coupled to said at least one of the transmitter and the receiver, wherein said at least one of the transmitter and the receiver is configured to send a key decryption request to the external agent when said external agent is coupled to said at least one of the transmitter and the receiver.

22. The system of claim 21, wherein the external agent is configured to respond to the key decryption request by decrypting each encrypted set of keys stored in said at least one of the transmitter and the receiver to generate at least one said set of private keys.

23. The system of claim 21, wherein the external agent is configured to respond to the key decryption request by sending information to said at least one of the transmitter and the receiver to enable said at least one of the transmitter and the receiver to decrypt each encrypted set of keys stored therein to generate at least one said set of private keys.

24. A transmitter for use in a communication system including said transmitter, a receiver, and a serial communication link between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol, wherein the protocol requires that each of the transmitter and receiver store a set of private keys, and process the private keys together with a value received from another element of the system to generate a shared secret, and wherein said transmitter includes:

a read-only memory which stores the private keys.

25. The transmitter of claim 24, wherein the transmitter includes shared secret generation circuitry, and the transmitter is configured so that said transmitter cannot be

operated in a mode in which substitute private keys are loaded into the shared secret generation circuitry instead of the private keys stored in the read-only memory.

26. A receiver for use in a communication system including said receiver, a transmitter, and a serial communication link between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol, wherein the protocol requires that each of the transmitter and receiver store a set of private keys, and process the private keys together with a value received from another element of the system to generate a shared secret, and wherein said receiver includes:

a read-only memory which stores the private keys.

27. The receiver of claim 26, wherein the receiver includes shared secret generation circuitry, and the receiver is configured so that said receiver cannot be operated in a mode in which substitute private keys are loaded into the shared secret generation circuitry instead of the private keys stored in the read-only memory.

28. A receiver for use in a communication system including said receiver, a transmitter, and a serial communication link between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol, wherein the protocol requires that the transmitter send a first distinctive value to the receiver during an authentication procedure, and that the receiver send a second distinctive value to the transmitter during the authentication procedure, and wherein said receiver includes:

circuitry for checking whether the first distinctive value that it receives during the authorization procedure satisfies at least one predetermined criterion, and to prevent authorization from succeeding if said first distinctive value does not satisfy each said criterion.

29. A transmitter for use in a communication system including said transmitter, a receiver, and a serial communication link between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol, wherein the protocol requires that the transmitter send a first distinctive value to the receiver during an authentication procedure, and that the

receiver send a second distinctive value to the transmitter during the authentication procedure, and wherein said transmitter includes:

circuitry for checking whether the second distinctive value that it receives during the authorization procedure satisfies at least one predetermined criterion, and to prevent authorization from succeeding if said second distinctive value does not satisfy each said criterion.

30. A receiver for use in a communication system including said receiver, a transmitter, and a serial communication link between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol, wherein the protocol requires that the transmitter and the receiver successfully complete an authentication exchange before the transmitter sends encrypted data to the receiver, and wherein said receiver includes:

lockout means configured to prevent successful completion of an authentication exchange between the receiver and the transmitter in the event that an authorization request is received at the receiver within a predetermined time window after a predetermined number of authentication requests have been received at the receiver.

31. A transmitter for use in a communication system including said transmitter, a receiver, and a serial communication link between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol, wherein the protocol requires that the transmitter and the receiver successfully complete an authentication exchange before the transmitter sends encrypted data to the receiver, and wherein said transmitter includes:

lockout means configured to prevent successful completion of an authentication exchange between the receiver and the transmitter in the event that an authorization request is received at the transmitter within a predetermined time window after a predetermined number of authentication requests have been received at the transmitter.

32. A communication system including:

a transmitter;

a receiver; and

a serial communication link between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a content protection

protocol, wherein the protocol requires that each of the transmitter and receiver store a set of private keys, and process the private keys together with a value received from an element of the system to generate a shared secret consisting of more than 56 bits, wherein each of the transmitter and the receiver is configured to generate the shared secret by generating a shared secret value consisting of more than 56 bits, wherein the shared secret value determines the shared secret.

33. A transmitter for use in a communication system including said transmitter, a receiver, and a serial communication link between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol, the protocol requires that each of the transmitter and receiver store a set of private keys and process the private keys together with a value received from an element of the system to generate a shared secret consisting of more than 56 bits, the transmitter is configured to generate the shared secret by generating a shared secret value consisting of more than 56 bits, the shared secret value determines the shared secret, and the transmitter includes:

a block module having six registers coupled and configured to receive a total of 168 parallel bits, the block module is a conventional HDCP-compliant block module, and the protocol is a modified version of the HDCP protocol in which the block module is used to generate the shared secret value so that said shared secret value consists of more than 56 bits but less than 104 bits.

34. A receiver for use in a communication system including said receiver, a transmitter, and a serial communication link between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol, the protocol requires that each of the transmitter and receiver store a set of private keys and process the private keys together with a value received from an element of the system to generate a shared secret consisting of more than 56 bits, the receiver is configured to generate the shared secret by generating a shared secret value consisting of more than 56 bits, the shared secret value determines the shared secret, and the receiver includes:

a block module having six registers coupled and configured to receive a total of 168 parallel bits, the block module is a conventional HDCP-compliant block module, and the protocol is a modified version of the HDCP protocol in which the block module

is used to generate the shared secret value so that said shared secret value consists of more than 56 bits but less than 104 bits.

35. A communication system including:

a transmitter;

a receiver; and

a serial communication link between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol, wherein the protocol requires that each of the transmitter and receiver store a set of private keys, and process the private keys together with a value received from another element of the system to generate a shared secret, wherein each of the transmitter and the receiver has a first configuration in which the shared secret is a first value and a second configuration in which the shared secret is a second value different than the first value.

36. The system of claim 35, wherein the protocol requires that each of the transmitter and receiver store a set of private keys, and process the private keys together with a value received from the other of the transmitter and the receiver to generate the shared secret.

37. The system of claim 35, wherein each of the transmitter and the receiver stores at least two selectable sets of the private keys, a first one of said selectable sets is selected in the first configuration and a second one of the selectable sets is selected in the second configuration.

38. A communication system including:

a transmitter;

a receiver;

a serial communication link between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol, wherein the protocol requires that each of the transmitter and receiver successfully complete an authentication exchange before the transmitter sends encrypted data to the receiver, the transmitter and the receiver are configured to exchange values during a first portion of the authentication exchange, and wherein

upon successful completion of the first portion of the authentication exchange, but only if the receiver is a repeater, the receiver sends authentication data to the transmitter during a second portion of the authentication exchange, wherein the authentication data is indicative of whether any unauthorized device is included in the system but is not indicative of any unencrypted value generated by the receiver during the first portion of the authentication exchange in response to the values sent to the receiver by the transmitter during said first portion of the authentication exchange.

39. A device for use in a communication system including a transmitter, a receiver, and a serial communication link between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol, the protocol requires that the receiver receive a pseudo-randomly generated value and that the receiver process said value during an initialization procedure, wherein the receiver must complete the initialization procedure before decrypting any encrypted data received over the link from the transmitter, wherein said device includes:

circuitry configured to generate the pseudo-randomly generated value in a manner employing a gaussian analog effect.

40. The device of claim 39, wherein the circuitry employs a diode-based white noise source to generate the pseudo-randomly generate value.

41. The device of claim 39, wherein the circuitry employs an R-C oscillator to generate the pseudo-randomly generate value.

42. A transmitter for use in a communication system including said transmitter, a receiver, and a serial communication link between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol, wherein the protocol requires that the transmitter send a pseudo-randomly generated value to the receiver before sending encrypted data to the receiver, and wherein said transmitter includes:

circuitry configured to generate the pseudo-randomly generated value in a manner employing a gaussian analog effect.

43. The transmitter of claim 42, wherein the circuitry employs a diode-based white noise source to generate the pseudo-randomly generate value.

44. The transmitter of claim 42, wherein the circuitry employs an R-C oscillator to generate the pseudo-randomly generate value.

45. A transmitter for use in a communication system including said transmitter, a receiver, and a serial communication link between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol, wherein the protocol requires that the transmitter send a pseudo-randomly generated value to the receiver before sending encrypted data to the receiver, and wherein the transmitter is configured so that said transmitter is not operable in any mode that allows substitution of an externally determined value for the pseudo-randomly generated value followed by transmission to the receiver of encrypted data that has been encrypted in a manner determined by the externally determined value.

46. A transmitter for use in a communication system including said transmitter, a receiver, and a serial communication link between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol in accordance with which the transmitter sends encrypted data to the receiver, and wherein said transmitter includes:

an input coupled to receive an input data stream; and

encryption circuitry for generating the encrypted data by encrypting the input data stream, wherein the transmitter is configured to detect whether the input data stream is an encrypted stream, and to operate the encryption circuitry to encrypt the input data stream only if said input data stream is not determined to be an encrypted stream.

47. A transmitter for use in a communication system including said transmitter, a receiver, and a serial communication link between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol in accordance with which the transmitter sends encrypted data to the receiver, and wherein said transmitter includes:

an input coupled to receive an input data stream; and

encryption circuitry for generating the encrypted data by encrypting the input data stream, wherein the transmitter is configured to detect whether the input data stream is data indicative of plain text, and to operate the encryption circuitry to encrypt the input data stream only if said input data stream is not determined to be data indicative of plain text.

48. A transmitter for use in a communication system including said transmitter, a receiver, and a serial communication link between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol in accordance with which the transmitter transmits encrypted data to the receiver, wherein the protocol requires that the receiver generate updated values during decryption of the encrypted data and send the updated values to the transmitter with predetermined timing, and wherein the transmitter is configured to cease transmission of the encrypted data to the receiver in the event that the transmitter does not receive the updated values with said predetermined timing.

49. A transmitter for use in a communication system including said transmitter, a receiver, and a serial communication link between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol in accordance with which the transmitter sends encrypted data to the receiver, wherein the protocol requires that the receiver transmit status information with predetermined timing to the transmitter during decryption of the encrypted data, and wherein the transmitter is configured to continue transmission of the encrypted data only after determining that the receiver has transmitted appropriate status information with the predetermined timing.

50. A transmitter for use in a communication system including said transmitter, a receiver, and a serial communication link between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol in accordance with which the transmitter sends encrypted data to the receiver, wherein the transmitter is configured to execute a re-authentication exchange with the receiver in response to predetermined circumstances following successful completion of an initial authentication exchange with the receiver, and the

transmitter is configured not to transmit non-degraded unencrypted data to the receiver during the re-authentication exchange.

51. The transmitter of claim 50, wherein said transmitter is configured to transmit degraded unencrypted data to the receiver during the re-authentication exchange.

52. A transmitter for use in a communication system including said transmitter, a receiver, and a serial communication link between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol in accordance with which the transmitter sends encrypted data to the receiver, wherein the transmitter is configured to execute a re-authentication exchange with the receiver in response to predetermined circumstances following successful completion of an initial authentication exchange with the receiver, and the transmitter is configured to transmit non-degraded, unencrypted data to the receiver only for a limited time commencing during the re-authentication exchange.

53. A transmitter for use in a communication system including said transmitter, a receiver, and a serial communication link between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol in accordance with which the transmitter sends encrypted data to the receiver, and wherein the transmitter includes:

an input coupled to receive an unencrypted data signal;

encryption circuitry coupled to the input, wherein the encryption circuitry is operable in a mode in which it generates the encrypted data from the unencrypted data signal; and

tamper protection circuitry configured to detect unauthorized tapping of the unencrypted data signal from the input.

54. A receiver for use in a communication system including said receiver, a transmitter, and a serial communication link between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol in accordance with which the transmitter sends encrypted data to the receiver over the link, and wherein the receiver includes:

decryption circuitry having an input coupled to receive the encrypted data and an output, wherein the decryption circuitry is operable in a mode in which it generates a decrypted data signal in response to the encrypted data and asserts the decrypted data signal at the output; and

tamper protection circuitry configured to detect unauthorized tapping of the decrypted data signal from the output.

55. A method for implementing a content protection protocol to encrypt data, said method including the steps of:

operating a transmitter to accept an unencrypted data signal, generate encrypted data in response to the unencrypted data signal in accordance with the content protection protocol, and send the encrypted data from the transmitter to a receiver over a serial link; and

while generating the encrypted data, detecting unauthorized tapping of the unencrypted data signal from the transmitter.

56. A method for implementing a content protection protocol to decrypt data, said method including the steps of:

operating a receiver to receive encrypted data transmitted to the receiver from a transmitter over a serial link, generating a decrypted data signal from the encrypted data in accordance with the content protection protocol, and asserting the decrypted data signal at an output of the receiver; and

while generating the decrypted data signal, detecting unauthorized tapping of the decrypted data signal from the transmitter.

57. A method for implementing a content protection protocol to encrypt data, said method including the steps of:

determining combinations of private key sets and key selection vectors, such that each of the private key sets together with one of the key selection vectors and a predetermined algorithm determines a shared secret; and

storing one of the private key sets and one of the key selection vectors in each of a set of transmitters and receivers, such that each of the transmitters together with any one of the receivers stores one of the combinations of private key sets and key selection vectors that determines the shared secret, but such that analysis of data

encrypted by the set of transmitters and receivers, together with the private key sets and the key selection vectors stored in the set of transmitters and receivers, cannot determine which one of the private key sets will generate the shared secret when processed with any known one of the key selection vectors in accordance with the algorithm.

58. A method for implementing a content protection protocol to encrypt data, said method including the steps of:

determining combinations of private key sets and key selection vectors, such that each of the private key sets together with one of the key selection vectors and a predetermined algorithm determines a shared secret; generating encrypted private key sets and encrypted key selection vectors by encrypting the private key sets and key selection vectors and delivering the encrypted private key sets and the encrypted key selection vectors to a facility; and

decrypting the encrypted private key sets and the encrypted key selection vectors at the facility to recover the private key sets and the key selection vectors, and storing one of the private key sets and one of the key selection vectors in each of a set of transmitters and receivers at the facility.

59. A method for implementing a content protection protocol to encrypt data, said method including the steps of:

(a) determining combinations of private key sets and key selection vectors, such that each of the private key sets together with one of the key selection vectors and a predetermined algorithm determines a shared secret, generating encrypted private key sets by encrypting the private key sets, and storing one of the encrypted private key sets in each transmitter and each receiver of a set of transmitters and receivers;

(b) delivering a device to a user, wherein said device is one of the set of transmitters and receivers; and

(c) after step (b), decrypting each of the encrypted private key sets stored in the device.

60. The method of claim 59, wherein step (a) also includes the steps of generating encrypted key selection vectors by encrypting the key selection vectors and storing one of the encrypted key selection vectors in said each transmitter and said each

receiver of the set of transmitters and receivers, and wherein step (c) also includes the step of decrypting each of the encrypted key selection vectors stored in the device.

61. A system, including:

transmitters and receivers configured to implement a content protection protocol, wherein the protocol requires that each of the receivers send authorization data to one of the transmitters during an authentication procedure, and the protocol requires each of the transmitters to prevent successful completion of the authorization procedure with one of the receivers when the authorization data sent to said one of the receivers includes a revocation value; and

an agent which stores a revocation list including each said revocation value, wherein at least one of the transmitters is configured to be coupled to the agent for sending to the agent a signal indicative of at least a portion of the authorization data received from one of the receivers, and wherein the agent is configured to check whether the authorization data indicated by the signal is indicative of any revocation value included in the revocation list.